POLYTECH NICE-SOPHIA

PROJET DE FIN D'ÉTUDE
2013 -2014

[E]

D1.1 - CAHIER DES CHARGES (DoW)

Sécurité dans un environnement ubiquitaire

Participant(s) :

- ABDELMESSIH, Fadi, fadi.william.ghali@gmail.com, IFI (IAM)
- JACQUELIN, Elie, elie.jacquelin@gmail.com, SI5 (IAM)
- ZOU, Enshuo, enshuo.zou@gmail.com, SI5 (IAM)
- TIGZIRI, Maxime, tigziri.maxime@gmail.com, IFI (CSSR)

Encadrant(s)

- BREL, Christian, brel@i3s.unice.fr, I3S (Rainbow)
- BOUDAOUD, Karima, karima@polytech.unice.fr, I3S (Rainbow)

Coût du livrable : [48h/étudiant] heures
Budget total du projet : [316h/étudiant + Encadrement] heures

Université Nice Sophia Antipolis

POLYTECH NICE-SOPHIA

Résumé Exécutif

L'objectif de ce projet est, dans un premier temps, d'implémenter une surcouche de sécurité au protocole UPnP afin de sécuriser l'échange de données entre des objets communiquant en assurant les trois propriétés de base de sécurité qui sont l'intégrité, confidentialité et authenticité. Dans un second temps, cette surcouche sera améliorée afin d'assurer l'authentification des utilisateurs des objets communicants. Cette couche sera ensuite testée en utilisant la plate-forme WComp sur un scénario basé sur des objets de la vie de tous les jours.

Abstract

The aim of this project is to, firstly, implement a security layer to the UPnP protocol to secure the data exchange between by ensuring the three basic properties of security, which are the integrity, the confidentiality and the authenticity. Secondly, this layer will be improved by implementing the authentication property. This layer will be tested on the WComp platform with a scenario using everyday life objects.

Table des matières

Description du Projet

Contexte de travail

De plus en plus d'objets connectés sont maintenant disponibles. Dans le cadre de la santé, nous travaillons sur un scénario basé sur des objets de la vie de tous les jours mais augmentés de capteurs.

Ces objets amènent alors dans l'environnement une possibilité d'interconnexion à travers l'exposition d'un ou plusieurs services et dans le cadre de la plateforme WComp, cette connexion s'appuie sur le protocole UPnP qui n'est pas sécurisé. Dans le cadre de ce projet, nous allons créer une couche de sécurité pour sécuriser le protocole de l'UPnP.

Motivations

Beaucoup d'objets qui font partie de notre quotidien sont connectés à Internet mais aussi entre eux et s'envoient des informations, des données. Si la connexion s'étendait à d'autres objets, des objets maintenant disponibles, sans écran, cela démocratisera l'Internet des objets. Il nous est toutes-fois utile de rappeler ce qu'est L'IoT (Internet of Things) :

Dans les années 1980, on parlait déjà « d'informatique ubiquitaire » cette dernière est basée sur des ordinateurs miniaturisés intégrés dans des objets variés qui accéderaient au Web et surferaient indépendamment d'une quelconque intervention humaine ; vers la fin des années 1990, Kevin Ashton, un pionnier des technologies RFID (Radio Frequency Identification), introduisit pour la première fois le terme « Internet des Objets » ou «Internet of Things» en anglais.

Internet est sans nul doute l'une des inventions les plus importantes et les plus significatives de toute l'histoire de l'humanité. On sait aussi l'impact qu'a déjà eu Internet sur l'enseignement, les communications, les entreprises, la science, les organismes publics et les hommes. Il faut se dire maintenant que la prochaine évolution d'Internet sera celle de l'IoT qui permettra d'améliorer considérablement sa capacité à rassembler, à analyser et à restituer des données que nous pourrons ensuite transformer en informations, en connaissances et enfin en savoir.

Capteurs → Données → Informations → Connaissances → Savoir

Ceci nous permettra d'optimiser, d'améliorer l'efficacité des infrastructures et de créer de nouveaux modèles commerciaux et nous récolteront, sous différentes formes, les principaux bénéfices de ce phénomène. La révolution des objets connectés a commencé et trouve déjà des applications concrètes dans plusieurs domaines, mais il reste que le défi essentiel à relever est la sécurisation de ces dispositifs en terme de protocoles et autres applicatifs. Nous nous attellerons, dans le cadre de ce projet, à sécuriser les communications entre les objets connectés. Pour cela, nous travaillerons sur un scénario basé sur des objets de la vie de tous les jours mais augmentés de capteurs dans un environnement d'interconnexion à travers l'exposition d'un ou plusieurs services et dans le cadre de la plateforme WComp, cette connexion s'appuie sur le protocole UPnP.

Ce dernier est un protocole qui apparaît extrêmement utile pour les utilisateurs lambda non-informaticiens qui ne veulent pas s'aventurer dans la configuration manuelle d'un équipement. Le protocole UPnP apporte donc une facilité et une simplification notable de l'informatique d'un point de vue utilisateur, cependant, ce protocole n'étant pas du tout sécurisé, notre objectif est de l'améliorer en sécurisant les flux de données échangées entres les objets communiquant et l'utilisateur.

Défis

Défi 1 : Sécurisation des communications et de l'environnement
Défi 2 : Authentification de l'utilisateur
Défi 3 : Intégrité de l'application

Objectif

Objectif 1 : Mettre en place un système de sécurité des communications entre les objets et les utilisateurs en assurant l'intégrité, la confidentialité et l'authenticité des données.
Objectif 2 : Mettre en place un système d'authentification des objets et des utilisateurs.
Objectif 3 : Mettre en place des tests qui assurent l'intégrité de l'application.

Scénario(s)

Dans ce projet, dans le cadre de la santé, nous travaillons sur un scénario basé sur des objets de la vie de tous les jours mais augmentés de capteurs.

Le scénario est le suivant :-

1. Bob achète un matelas communicant. Ce matelas composé de capteurs de pression permet de connaître la position de la personne sur le matelas. Ces données sont supervisées à travers des applications dédiées.

2. Bob achète une lampe communicante. La lampe en plus d'assurer sa fonction primaire est composée d'un capteur sonore. Les données provenant de ce capteur ainsi que son état (allumée ou éteinte) sont aussi supervisées à travers des applications dédiées.

3. Bob apporte dans sa chambre son (Smartphone). Celui-ci est composé entre autre d'une application Réveil. Lorsque Bob active le réveil, la lampe qui était allumée, s'éteint alors au bout de quelques secondes.

4. Bob achète un chargeur de téléphone communiquant. Ce chargeur est composé d'un petit mur de led et d'un certains nombres de capteurs (luminosité, température, qualité de l'air etc...). Toutes ces données sont alors supervisées à travers une application dédiée. De plus, lorsque le téléphone est branché sur le chargeur, la lampe qui était allumée, s'éteint et le mur de led du chargeur prend le relai et s'allume. Lorsque Bob active son réveil, alors le mur de led s'éteint automatiquement au bout de quelques secondes.

Dans le cadre de ce scénario, nous allons sécuriser l'échange de données entre les objets communicants en assurant les trois propriétés de base de sécurité qui sont l'intégrité, la confidentialité et l'authenticité. Puis, nous rajouterons la propriété d'authentification de l'utilisateur.

Critères de succès

Critère 1 : Les messages entre les objets et avec l'utilisateur sont bien sécurisés.
Critère 2 : L'authentification des utilisateurs et des objets est bien assurée.
Critère 3 : L'application est sécurisée.

Etat de l'art

Description Générale

Un environnement ubiquitaire est un environnement où l'informatique est omniprésente. Pour que cela soit possible, l'utilisation d'objets communicants est primordiale : ces objets de la vie quotidienne récupèrent des informations sur l'utilisateur ou son environnement et les communiquent à d'autres objets pour analyser ces données. Notre projet consiste à sécuriser cette communication, celui-ci repose sur différentes parties :

- Le protocole UPnP (Universal Plug and Play)
- La propriété d'authenticité des données.
- La propriété de confidentialité des données.
- La propriété d'intégrité des données.
- la propriété d'authentification de l'utilisateur.
- La plateforme WComp

La confidentialité, l'intégrité et l'authenticité sont les trois propriétés de base de sécurité. La propriété de confidentialité permet de protéger le contenu lors de la communication sur un réseau ou lors du stockage des données. Seulement les personnes autorisées peuvent accéder et lire des données sécurisées. Le chiffrement de données permet de résoudre le problème de confidentialité de données. La propriété d'intégrité assure que les données reçues sont identiques aux données envoyées, c'est-à-dire, les données ne doivent pas être modifiées lors de la transmission. Les algorithmes de hachage, le condensé de message, la signature numérique protègent l'intégrité de données. La propriété d'authenticité s'applique à deux cas: soit aux personnes soit aux documents. L'authenticité d'une personne est la garantie que la personne est bien celle qu'elle prétend être. Quant à un document, l'authenticité vise à prouver l'origine du document.

Ces propriétés de sécurité doivent être fournies par un protocole de communication afin d'assurer un échange de données sécurisé entre les objets communicants. Dans le cadre de ce projet, l'échange de données se fera via le protocole UPnP qui est le plus utilisé.

L'UPnP

Le protocole UPnP (Universal Plug and Play) est un protocole développé au début des années 2000 grâce à l'association de plusieurs compagnies d'informatique majeures.

Ce protocole a pour but de mettre en réseau différent terminaux dans un réseau généralement à petite échelle comme une maison. Une fois la communication rendue possible, les différents terminaux peuvent être contrôlés à distance.

Une application possible de l'UPnP est un serveur média pouvant être contrôlé par d'autres terminaux pour lancer une musique ou un film.

L'UPnP se base sur plusieurs protocoles dans son fonctionnement (HTTP, TCP/IP, UDP, SOAP, …) et une communication via UPnP suit plusieurs étapes :

1. Découverte : quand un terminal est branché au réseau, il parcourt celui-ci pour découvrir quelles sont les autres terminaux utilisant UPnP à l'aide du protocole SSDP

(Simple Service Discovery Protocole) : un échange de messages se fait entre le nouveau terminal et ceux déjà présents, ces messages contiennent une identification du terminal contenant une URL vers un description de celui-ci.

2. Description : à partir de l'URL obtenu dans la découverte, le terminal a accès à un fichier XML décrivant tout les services disponibles pour pouvoir contrôler le terminal par la suite.
3. Contrôle : grâce au fichier reçu précédemment, il est possible de contrôler le terminal (ex : lancer une musique) en utilisant le protocole SOAP sur une URL décrit dans le fichier XML. Le terminal contrôlé va répondre en décrivant l'état actuel du service.

Notification d'évènements : après une action, les variables du terminal qui l'a effectué sont modifiés, le service peut être potentiellement changé avec ces nouvelles valeurs de variables. Il va donc émettre une notification à tous les autres terminaux abonnés à ce service pour les informer de ce changement.

Le problème de ce protocole est qu'il n'y a aucune mention de sécurité : n'importe quel terminal, tant qu'il est connecté au réseau, peut contrôler n'importe quel terminal sous protocole UPnP sans permissions préalable (principe d'authenticité), il est possible aussi de récupérer les messages envoyés d'un terminal à un autre car le message n'est pas crypté (principe de confidentialité) et enfin il n'est pas assuré que le message reçu n'a pas été modifié (principe d'intégrité).

L'UPnP étant un protocole très utilisé dans un environnement ubiquitaire, il faut donc le sécuriser.

Une des manières de rendre cela possible est de sécuriser un des protocoles "racines" sur lequel la communication de l'UPnP est basé : HTTP, TCP/IP, UDP.

Le papier, "A Security-Property-Based Approach for lowering Power Consumption of Secure Mobile Web Access"[1], décrit un protocole HTTP modifié sécurisé par l'intermédiaire d'un proxy, ce protocole requiers peu de ressources ce qui est un avantage dans les objets communicants où les ressources sont limités.

Ce protocole HTTP assure les propriétés de bases de sécurité : authenticité, confidentialité et intégrité.

Propriété d'Authenticité des objets

Comme nous l'avons dit précédemment, l'authenticité concerner soit les messages ou les personnes :

1. Dans le cadre d'un message, l'authenticité doit garantir qu'il est possible de déterminer avec précision l'origine de celui-ci.
2. Dans le cadre d'une personne, l'authenticité doit garantir que la personne est bien celle qu'elle prétend être.

Après avoir défini la propriété d'authenticité, nous allons maintenant définir les deux autres propriétés de confidentialité et d'intégrité.

Propriété de confidentialité

Pour assurer la propriété de confidentialité il faut que le message transmis ne soit compréhensible que par l'expéditeur et le destinataire du message.

Cette propriété est assurée grâce au principe de chiffrement qui peut être symétrique ou asymétrique.

Chiffrement symétrique

L'expéditeur et le récepteur ont une même clé permettant de chiffrer et déchiffrer des données. Le chiffrement symétrique utilise un algorithme de chiffrement léger qui prend beaucoup moins de temps qu'un algorithme de chiffrement asymétrique. Pour ce type de chiffrement, on n'a besoin que d'une clé pour chiffrer et déchiffrer les messages. Mais l'inconvénient de la cryptographie symétrique est l'exigence d'une clé secrète partagée, avec une copie à chaque extrémité. Par exemple, pour n personnes dans un réseau, afin de sécuriser les communications entre eux. On a besoin d'un nombre de clés de jusqu'à n(n-1)/n. Afin de diminuer la probabilité d'une découverte éventuelle de clef par un tiers, elles doivent être changées régulièrement et conservées en lieu sûr. Le processus de gestion des clés (sélection, distribution et stockage des clés) est difficile à réaliser de manière fiable et sécurisée.

Chiffrement asymétrique

Dans la cryptographie asymétrique, la clé pour chiffrer les messages est différente de la clé pour déchiffrer les messages. Chaque utilisateur possède une paire de clés, une clé publique et une clé privée. La clé privée doit rester confidentielle, elle doit être connue uniquement par son propriétaire. La clé publique est accessible par tout le monde. Les messages à envoyer sont chiffrés par la clé publique du récepteur. Les messages chiffrés ne peuvent qu'être déchiffrés par la clé privée correspondante. La procédure de chiffrement et déchiffrement est comme suit:

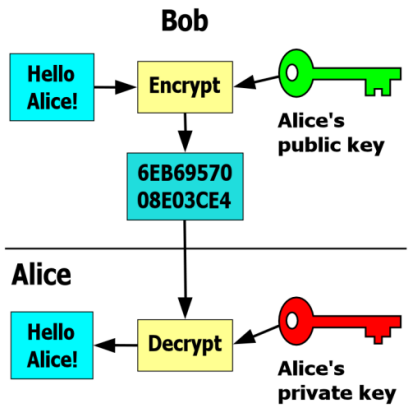


Figure : Cryptographie asymétrique (Source: http://en.wikipedia.org/wiki/File:Public_key_encryption.svg)

Le problème de cryptographie asymétrique est la « lourdeur » de l'algorithme de chiffrement/déchiffrement.

La solution pour résoudre ce problème est d'utiliser la cryptographie symétrique pour sécuriser la communication et utiliser la cryptographie asymétrique pour communiquer la clé symétrique.

Propriété d'intégrité

La propriété d'intégrité impose que le message ne soit pas modifié lors de son envoi entre l'expéditeur et le destinataire. Pour assurer cette propriété, un hash est ajouté au message à envoyer, grâce à une fonction de hachage. Le message ainsi que son hash sont envoyés ensemble.

Hachage

Une fonction de hachage est une fonction qui prend une chaîne de données de longueur quelconque et renvoie une chaîne de données de longueur fixée. La valeur renvoyée est nommée l'empreinte ou le condensé. Le sens de hachage est unique, c'est-à-dire c'est très difficile à inverser le résultat de hachage pour revenir l'origine de données. Du coup, ce n'est pas comme une technique de chiffrement. On ne peut pas trouver deux messages différents ayant le même résultat de hachage. Il y a deux fonctions de hachage plus utilisées qui sont les MD5 et le SHA.

Après avoir définis les trois propriétés de base (authenticité, confidentialité et intégrité) qui seront implémentés au dessus du protocole UPnP afin de sécuriser les communications dans un environnement ubiquitaire, nous allons maintenant définir la plateforme WComp utilisée dans le cadre de ce projet pour configurer des objets communicants.

WComp

WComp est un environnement de prototypage pour faciliter le développement dans un environnement ubiquitaire, créé par l'équipe Rainbow du laboratoire I3S de l'université de Nice-Sophia Antipolis.

L'architecture de WComp repose sur deux éléments :

Containers : ils permettent de gérer les différentes phases de vie d'un composant (instanciation, destruction, ..) et d'être une interface pour gérer le composant.

Designers : ils permettent de manipuler et adapter les containers, de sélectionner les actions à effectuer.

Un avantage de WComp est d'abstraire la communication entre composants pour permettre un prototypage rapide sans se soucier d'intégrer un composant particulier.

Méthodologie et Planification

Stratégie Générale

Pour mener à bien ce projet, nous avons choisie une stratégie linéaire. Nous commencerons par étudier les travaux existants, en particulier la plateforme WComp, UPnP ainsi que les composants de sécurité. Nous implémenterons ensuite une surcouche au dessous de UPnP avec les composants de sécurité permettant d'assurer les propriétés de sécurité éponymes. Enfin, nous finirons avec des tests que nous réaliserons sur le scénario défini précédemment.

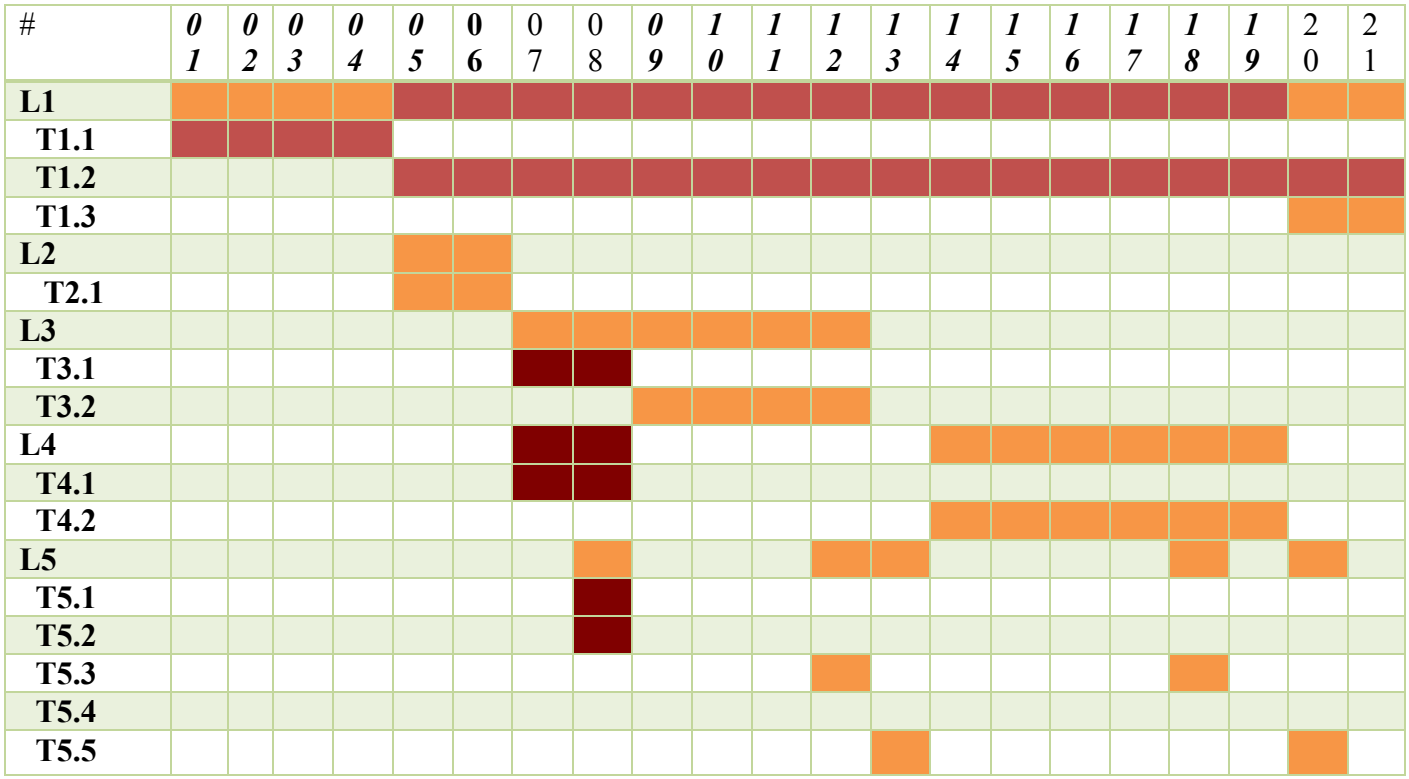
Le lot L1 sera consacré au suivi du projet, l'organisation des réunions le long du projet, la réalisation du diaporama et de la vidéo de démonstration du projet. Le lot L2, ce lot sera consacré à l'étude préliminaire des travaux existants avant de commencer l'implémentation. Les lots L3 et L4, seront consacrés à l'implémentation (écriture du code). Finalement, le lot L5, sera consacré au test de l'implémentation et du protocole UPnP sécurisé grâce à la surcouche de sécurité

Découpage en lots

#	Titre du lot	Type	Leader	Budget	Début	Fin
L1	Management du projet	MGMT	ABDELMESSIH	538h	S1	S21
L2	Étude préliminaire	RECH	TIGZIRI	88h	S5	S6
L3	Sécurité des communications	IMPL	JACQUELIN	244h	S7	S12
L4	Authentification	IMPL	ABDELMESSIH	244h	S7	S19
L5	Test	IMPL	ZOU	421h	S13	S20
			Total :	[316h/étudiant]		

Tableau 1 - Liste des Lots

Planification



Quatre personnes **Une personne** **Deux personnes**

Figure 1 - Diagramme de Gantt

Livrables associés au projet

#	Titre du livrable	Lot	Nature	Date
D1.1	Cahier des charges (DoW)	1	DOC	S4
D1.2	Rapport de Management (MGMT)	1	DOC	S21
D1.3	Diaporama de la présentation finale	1	DOC	S21
D2.1	Rapport de faisabilité et d'implémentation du projet	2	DOC	S6
D3.1	Code de mise en œuvre de confidentialité	3	LOG	S8
D3.2	Code de mise en œuvre d'intégrité	3	LOG	S12
D4.1	Code de mise en œuvre d'authentification des objets communicants	4	DOC	S8
D4.2	Code de mise en œuvre d'authentification des utilisateurs	4	LOG	S19
D5.1	Rapport des tests réalisés	5	DOC	S20
D5.2	Code de mise en œuvre du projet réunifié	5	LOG	S20

Tableau 2 - Liste des livrables

Jalons

#	Titre du jalon	Lot(s)	Date	Vérification
J1	Fin de la phase de planification initiale du projet	1	S4	D1.1 livré.
J2	Fin de l'étude préliminaire	2	S6	D2.1 livré
J3	Fin de la mise en œuvre du code de confidentialité	3	S8	D3.1 livré
J4	Fin de la mise en œuvre du code d'intégrité	3	S12	D3.2 livré
J5	Fin de la mise en œuvre du code d'authentification des objets communicants	4	S8	D4.1 livré
J6	Fin de la mise en œuvre du code d'authentification des utilisateurs	4	S19	D4.2 livré
J7	Fin du rapport des tests réalisés	5	S20	D5.1 livré
J8	Fin de la mise en œuvre du code du projet réunifié	5	S20	D5.2 livré
J9	Fin du projet et du rapport du management	1	S21	D1.2 livré
J10	Fin du diaporama de la présentation finale	1	S21	D1.3 livré

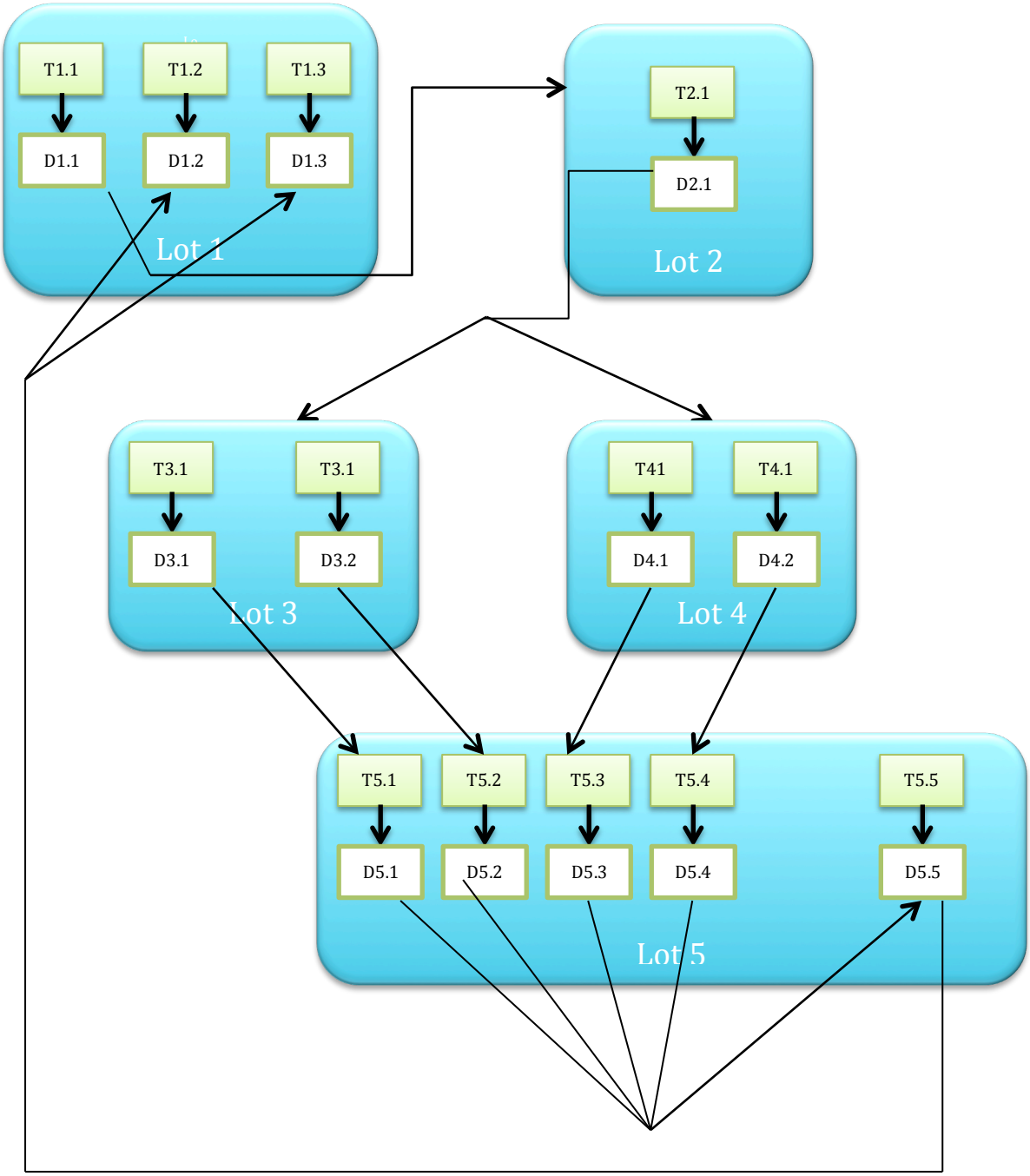
Tableau 3 - Liste des jalons

Pilotage et suivi

Dans ce projet, le suivi du projet est assuré par nos encadrants. Durant la planification du projet, nous avons prévu une réunion pour les semaines à temps partiel et deux réunions pour les semaines à temps plein. En plus, pour chaque lot et pour chaque tâche, il y a un responsable qui s'assure du bon déroulement du travail.

Description de la mise en œuvre du projet

Interdépendances des lots et tâches



Description des lots

Identifiant	L1		Date de démarrage	S1		
Titre	Management du projet					
Type	MGMT					
Participant	ABDELMESSIH	JACQUELIN	ZOU	TIGZIRI	BREL	BOUDAOUD
Effort	120	120	120	120	29	29

Objectifs du lot

- Planification du projet.
- Suivi du projet et les réunions avec les encadrants.
- Rédaction du rapport de management.
- Préparation de soutenance.

Description du lot

Tâche T1.1 : Planification (ABDELMESSIH, S1 - S4, 192h)

Cette tâche consiste à étudier et comprendre le projet, déterminer la stratégie du travail, planifier les lots, les tâches, jalons et les livrables et consiste à planifier la répartition du travail entre les membres du projet.

Tâche T1.2 : Suivi de projet (ABDELMESSIH, S5 - S21, 174h)

Cette tâche consiste à suivre l'évolution du projet, assurer le succès du projet et la réalisation des tâches des lots. Cela implique la livraison des livrables suivant le temps indiqué dans le DoW et tenir compte des jalons et des critères de succès. Cette tâche consiste aussi à gérer les risques et à trouver des solutions aux problèmes rencontrés. Les réunions avec les encadrants sont également gérées dans cette tâche.

Tâche T1.3 : Démonstration et diaporama (ABDELMESSIH, S20 - S21, 172h)

Cette tâche consiste à faire un diaporama qui présente le travail réalisé durant du projet et une vidéo de démonstration.

Livrable

Livrable D1.1 : Cahier des charges (ABDELMESSIH, DOC, S4)

Ce livrable consiste à rendre le document qui décrit la planification du projet ainsi que la répartition en lots, tâches, jalons et livrables. Ce document sert aussi à montrer la répartition du travail entre les membres du projet. Tâche : T1.1

Livrable D1.2 : Rapport de management (ABDELMESSIH, DOC, S21)

Ce livrable consiste à rendre un document de management qui sert à suivre l'évolution du projet et s'assure de la réalisation du travail indiqué dans le DoW. Il sert également à décrire la gestion des risques et des difficultés le long du projet. Tâche : T1.2

Livrable D1.3 : Diaporama de la présentation finale (ABDELMESSIH, DOC, S21)

Ce livrable consiste à rendre le diaporama qui représente le travail réalisé le long du projet et de faire une vidéo de démonstration. Tâche : T1.3

Identifiant	L2		Date de démarrage		S5	
Titre	Étude préliminaire					
Type	RECH					
Participant	ABDELMESSIH	JACQUELIN	ZOU	TIGZIRI	BREL	BOUDAOUD
Effort	22	22	22	22		

Objectifs du lot

- Étude des solutions existantes et des choix d'implémentation.

Description du lot

Tâche T2.1 : Étude de faisabilité et d'implémentation du projet (TIGZIRI, S5 - S 6, 88h)

Cette tâche consiste à étudier les solutions existantes et les choix d'implémentation.

Livrable

Livrable D2.1 : Rapport de faisabilité et d'implémentation du projet (TIGZIRI, DOC, S6)

Ce livrable consiste à rendre un document qui compare et décrit les solutions existantes ainsi que les choix d'implémentation. Tâche : T2.1

Identifiant	L3		Date de démarrage		S7	
Titre	Sécurité des communications					
Type	IMPL					
Participant	ABDELMESSIH	JACQUELIN	ZOU	TIGZIRI	BREL	BOUDAOUD
Effort	33	89	33	89		

Objectifs du lot

- Assurer la confidentialité des données.
- Assurer l'intégrité des données.

Description du lot

Tâche T3.1 : Implémentation du code de la confidentialité (JACQUELIN, S7 - S8, 112h)

Ecriture du code permettant d'assurer la confidentialité des données.

Tâche T3.2 : Implémentation du code de l'intégrité (ZOU, S9 - S12, 132h)

Ecriture du code permettant d'assurer l'intégrité des données.

Livrable

Livrable D3.1 : Code de mise en œuvre de la confidentialité (JACQUELIN, LOG, S8)

Ce livrable consiste à implémenter le code permettant d'assurer la confidentialité des données.
Tâche : T3.1

Livrable D3.2 : Code de mise en œuvre d'intégrité (ZOU, LOG, S12)

Ce livrable consiste à implémenter le code permettant d'assurer l'intégrité des données.
Tâche : T3.2

Identifiant	L4		Date de démarrage	S7		
Titre	Authenticité et Authentification					
Type	IMPL					
Participant	ABDELMESSIH	JACQUELIN	ZOU	TIGZIRI	BREL	BOUDAOUD
Effort	89	33	89	33		

Objectifs du lot

- Assurer l'authenticité des données échangées entre les objets communicants.
- Permettre l'authentification des utilisateurs.

Description du lot

Tâche T4.1 : Implémentation du code pour l'authenticité des données (ABDELMESSIH, S7 – S8, 112h)

Ecriture du code permettant d'assurer l'authenticité des données.

Tâche T4.2 : Implémentation du code de l'authentification des utilisateurs
(TIGZIRI, S14 – S19, 132h)

Ecriture du code permettant d'assurer d'authentification des utilisateurs.

Livrable

Livrable D4.1 : Code de mise en œuvre de l'authenticité (ABDELMESSIH, DOC, S8)

Ce livrable consiste à implémenter permettant d'assurer l'authenticité des données. Tâche : T4.1

Livrable D4.2 : Code de mise en œuvre de l'authentification des utilisateurs (TIGZIRI, LOG, S19)

Ce livrable consiste à implémenter le code d'authentification des utilisateurs. Tâche : T4.2

Identifiant	L5		Date de démarrage		S8	
Titre	Tests et réunification du projet					
Type	IMPL					
Participant	ABDELMESSIH	JACQUELIN	ZOU	TIGZIRI	BREL	BOUDAOUD
Effort	103	103	103	103		

Objectifs du lot

- Tester les résultats des implémentations du Lot 3 et 4.
- Réunification du travail du projet.

Description du lot

Tâche T5.1 : Test de fonctionnalité du code d'authenticité des données
(ABDELMESSIH, S8, 40h)

Cette tâche consiste à tester le code d'authenticité des données et de modifier ce code si nécessaire

Tâche T5.2 : Test de fonctionnalité du code d'intégrité des données
(JACQUELIN, S8, 40h)

Cette tâche consiste à tester le code d'intégrité des données et de modifier ce code si nécessaire.

Tâche T5.3 : Test de fonctionnalité du code de confidentialité des données
(ZOU, S12, 44h)

Cette tâche consiste à tester le code de confidentialité des données et de modifier ce code si nécessaire.

Tâche T5.4 : Test de fonctionnalité du code d'authentification des utilisateurs
(TIGZIRI, S18, 44h)

Cette tâche consiste à tester le code d'authentification des utilisateurs et de modifier ce code si nécessaire.

Tâche T5.5 : Réunification et test d'intégrité de l'application
(JACQUELIN, S13 et S20, 232h)

Cette tâche consiste à réunifier les codes d'implémentation du projet, de tester l'intégrité de l'application sur le scénario du projet et de corriger le code si nécessaire.

Livrable

Livrable D5.1 : Rapport des tests réalisés (ZOU, DOC, S20)

Ce livrable contient les rapports décrivant les tests effectués de toutes les tâches du lot.

Livrable D5.1 : Code de mise en œuvre du projet réunifié (ZOU, LOG, S20)

Ce livrable consiste à rendre le code du projet réunifié qui contient l'implémentation de la couche de sécurité et l'implémentation du scénario. Tâche : T5.5

Résumé de l'effort

	ABDELMESSIH	JACQUELIN	ZOU	TIGZIRI	BREL	BOUDAOUD
L1 - Management						
T1.1 - Planification	48	48	48	48		
T1.2 - Suivi de projet	29	29	29	29	29	29
T1.3 - Démonstration	43	43	43	43		
Sous-Total (h) :	**120**	**120**	**120**	**120**	**29**	**29**
L2 - Étude préliminaire						
T2.1 - Étude de faisabilité et d'implémentation du projet	22	22	22	22		
Sous-Total (h) :	**22**	**22**	**22**	**22**		
L3 - Sécurité des communications						
T3.1 - Implémentation du code de la confidentialité		56		56		
T3.2 - Implémentation du code de l'integrité	33	33	33	33		
Sous-Total (h) :	**33**	**89**	**33**	**89**		
L4 - Authentification						
T4.1 - Implémentation du code de l'authentification des objets communicants	56		56			
T4.2 - Implémentation du code de l'authentification des utilisateurs	33	33	33	33		
Sous-Total (h) :	**89**	**33**	**89**	**33**		
L5 - Tests et réunification du projet						
T5.1 - Test de fonctionnalité du code d'authenticité des objets	20		20			
T5.2 - Test de fonctionnalité du code d'intégrité de la communication utilisateurs		20		20		
T5.2 - Test de	11	11	11	11		

fonctionnalité du code de confidentialité de la communication						
T5.3 - Test de fonctionnalité du code d'authenticité des utilisateurs	11	11	11	11		
T5.4 - Réunification et test d'intégrité de l'application	58	58	58	58		
Sous-Total (h) :	**100**	**100**	**100**	**100**		
Total (h) :	**364**	**364**	**364**	**364**	**29**	**29**

Tableau 4 - Résumé de l'effort

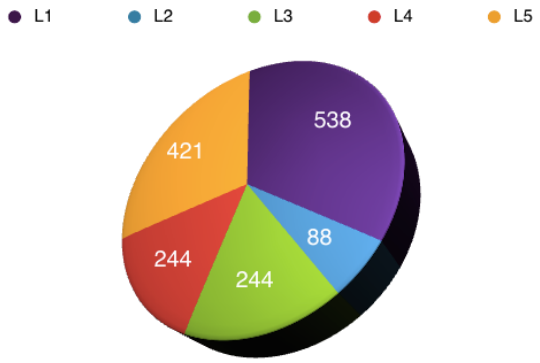


Figure 2 - Répartition de l'effort par lot (heures)

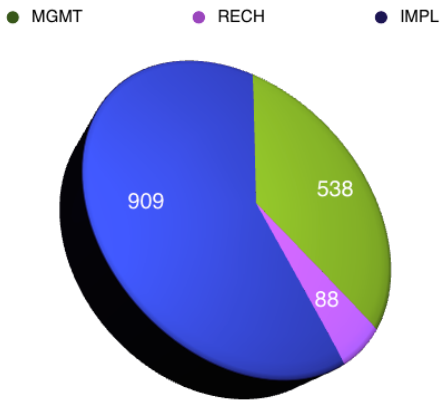


Figure 3 - Répartition de l'effort par type (heures)

Gestion du risque

Description	Probabilité	Conséquences	Impact	Cause	Évitement	Résolution
Communication difficile à sécuriser	Moyen (30 %)	Plus de travail	Retard sur les lots concernés	Temps alloué insuffisant	Travail de recherche préliminaire efficace	Revoir la méthode utilisée
Objets communiquant non fonctionnel	Faible (20 %)	Scénario invalide et tests non réalisables	Retard	Défaut de fabrication / mauvaise utilisation	Avoir du matériel de rechange	Changer le scénario / objet
Pas d'implémentation d'algorithmes existants	Faible (10 %)	Scénario invalide et tests non réalisables	Retard	Indisponibilité	Travail de recherche préliminaire efficace	Trouver des alternatives / Réaliser l'implémentation

Tableau 5 - Table de gestion des risques

Participants

Fadi ABDELMESSIH (M2 - IAM)

A la suite de son étude à l'Université Française d'Egypte (UFE) dans le domaine de la technologie de l'information et de la communication (TIC) option systèmes embarqués. Dans le cadre de ce master, Fadi termine son diplôme d'ingénierie égyptien et en même temps le master 2 Ingénierie et Fondements de l'Informatique parcours Informatique Ambiante et Mobile (IAM) grâce à un partenariat l'université Nice Sophia Antipolis.
Dans ce projet, en tant qu'un étudiant IAM qui prend des cours à tous ce qui concerne la mise en œuvre des objets dites communicants. Il sera en charge en charge de la mise en œuvre de la composante qui implémente l'authentification des objets communicants mais aussi du management du projet et de la présentation finale du projet.

Elie JACQUELIN (SI5 - IAM)

Après être passé par une classes préparatoire, Elie a rejoint le cycle ingénieur en informatique à Polytech'Nice-Sophia. Le parcours Informatique Ambiante et Mobile (IAM) qu'il suit proposé un cours intitulé "objets communicants" qui explique a mise en œuvre d'objets communicants qui font partie intégrante d'un environnement ubiquitaire, ce qui l'aidera à mettre en œuvre les protocoles créer durant ce projet.
Il sera en charge de la création d'une des propriétés de sécurité mais aussi de la réunification de toutes les autres propriétés.

Maxime TIGZIRI (M2 – CSSR)

Après des études en architecture réseaux et systèmes, j'ai rejoint le cycle Master-2 en cryptographie, systèmes, sécurité et réseaux (CSSR) informatique à Polytechniques Nice-Sophia-Antipolis. Le parcours cryptographie, systèmes, sécurité et réseaux (CSSR) que je suis, propose un cours qui fait l'étude et la mise en œuvre des objets dits communicants (ou Internet of Things) dans un environnement ubiquitaire et l'analyse de leurs évolutions vers des solutions de plus en plus spécifiques. Aux termes de ce projet nous aurons, mes collaborateurs et moi-même, mis au point des solutions garantissant les trois grands principes de la sécurité, à savoir l'authentification, l'intégrité et la disponibilité et répondant aux normes ISO.

Enshuo ZOU (SI5 – IAM)

Ayant obtenu une licence de génie informatique à l'université de Shanghai en Chine, j'ai choisi de continuer mes études à l'école d'ingénieur Polytech'Nice Sophia-Antipolis. Cette année, j'ai choisi de m'inscrire au parcours Informatique Ambiante et Mobile où je suis le cours objet communicants concernant la création des objets communicants et l'utilisation du protocole UPnP. Dans ce projet, je serai en charge de la création des propriétés de sécurité et les tests de la fonctionnalité.

Christian Brel (Ingénieur de Recherche - Equipe Rainbow, Laboratoire I3S - UNS/CNRS)

Ayant soutenu ma thèse en Juin 2013 sur la composition d'applications dirigée par les interfaces hommes-machines, j'ai maintenant un poste d'Ingénieur de Recherche lié à un projet basé sur des objets communicants. Par conséquent, j'ai des compétences sur le framework WComp permettant de mettre en place rapidement des prototypes d'applications mettant en jeux des objets communicants. Ce projet est basé sur l'utilisation d'objets de la vie quotidienne augmentés de capteurs, pour créer une application répondant à un besoin de prévention santé. C'est dans ce cadre que je suis intéressé par ce PFE qui doit permettre d'identifier les personnes manipulant les objets afin de mieux préciser le monitoring effectué sur chacun des objets de l'application.

Karima Boudaoud (Ingénieur de Recherche - Equipe Rainbow, Laboratoire I3S - UNS/CNRS)

Karima Boudaoud est maître de conférences à l'Université de Nice Sophia Antipolis (UNSA), depuis 2002. Elle fait ses recherches au laboratoire I3S-CNRS/UNSA dans le projet Rainbow et enseigne au département RT de l'IUT de Nice Côte d'Azur. Ses intérêts de recherche sont les suivants: gestion de la vie privée, gestion de la sécurité, la cybercriminalité, les politiques de sécurité, détection d'intrusion, backtracking, les systèmes multi-agents, la sécurité des applications à base de composants, de la sécurité du transfert de documents électroniques, de la sécurité dans les environnements ubiquitaires et Cloud.

Bibliographie & Références

[1] C. Pita, K. Boudaoud, M. Riveill, “A Security-Property-Based Approach for lowering Power Consumption of Secure Mobile Web Access”, IWCMC, 2011

[2] “Securing Application Layer Protocols by Assembling Security Components”, Cosmin Pita, 2009

[3] “Site de WComp”, http://www.wcomp.fr/